SC-300 Q&As

Microsoft Identity and Access Administrator

QUESTION 1

HOTSPOT

You have a Microsoft 365 tenant.

You need to Identity users who have leaked credentials. The solution must meet the following requirements:

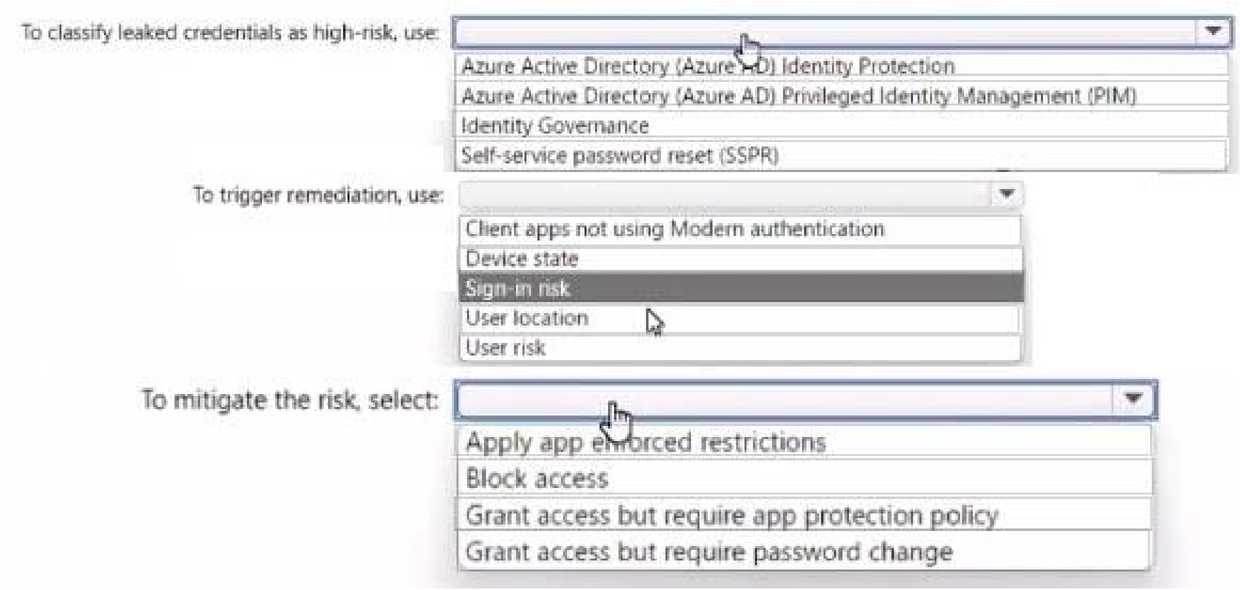
Identity sign-ms by users who are suspected of having leaked credentials.

Flag the sign-ins as a high-risk event.

Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

What should you use? To answer, select the appropriate options m the answer area.

Hot Area:



To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

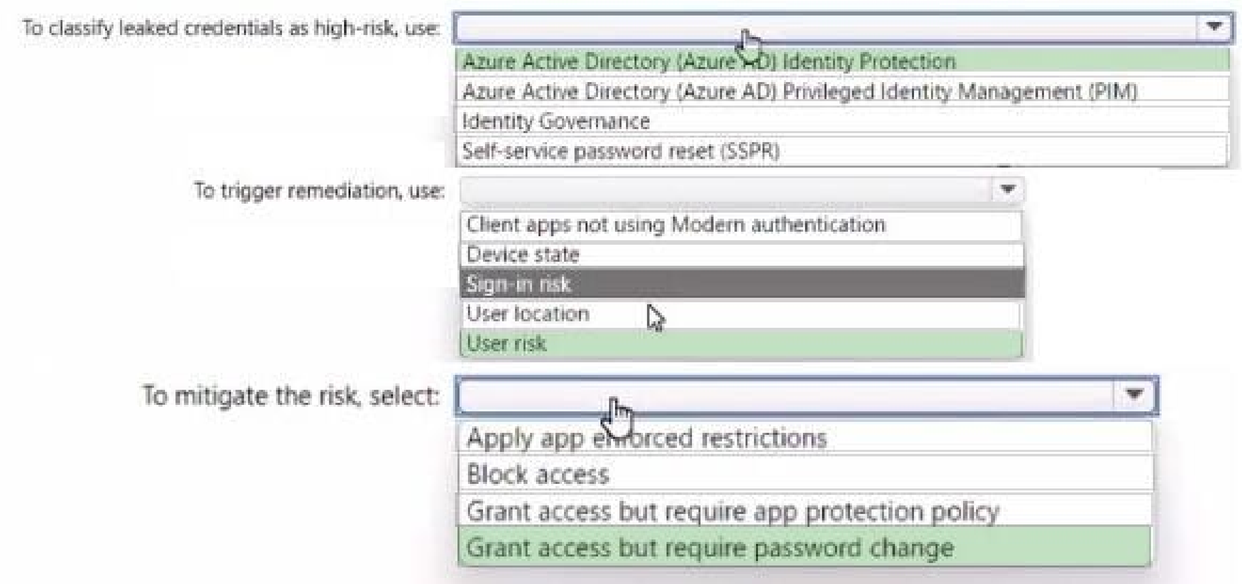
To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Correct Answer:



To classify leaked credentials as high-risk, use:

- [✓ Azure Active Directory (Azure AD) Identity Protection]
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

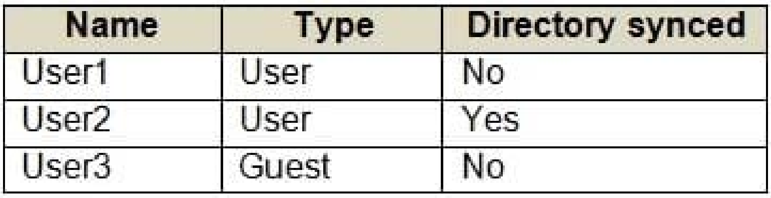
- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- [✓ User risk]

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- [✓ Grant access but require password change]

QUESTION 2

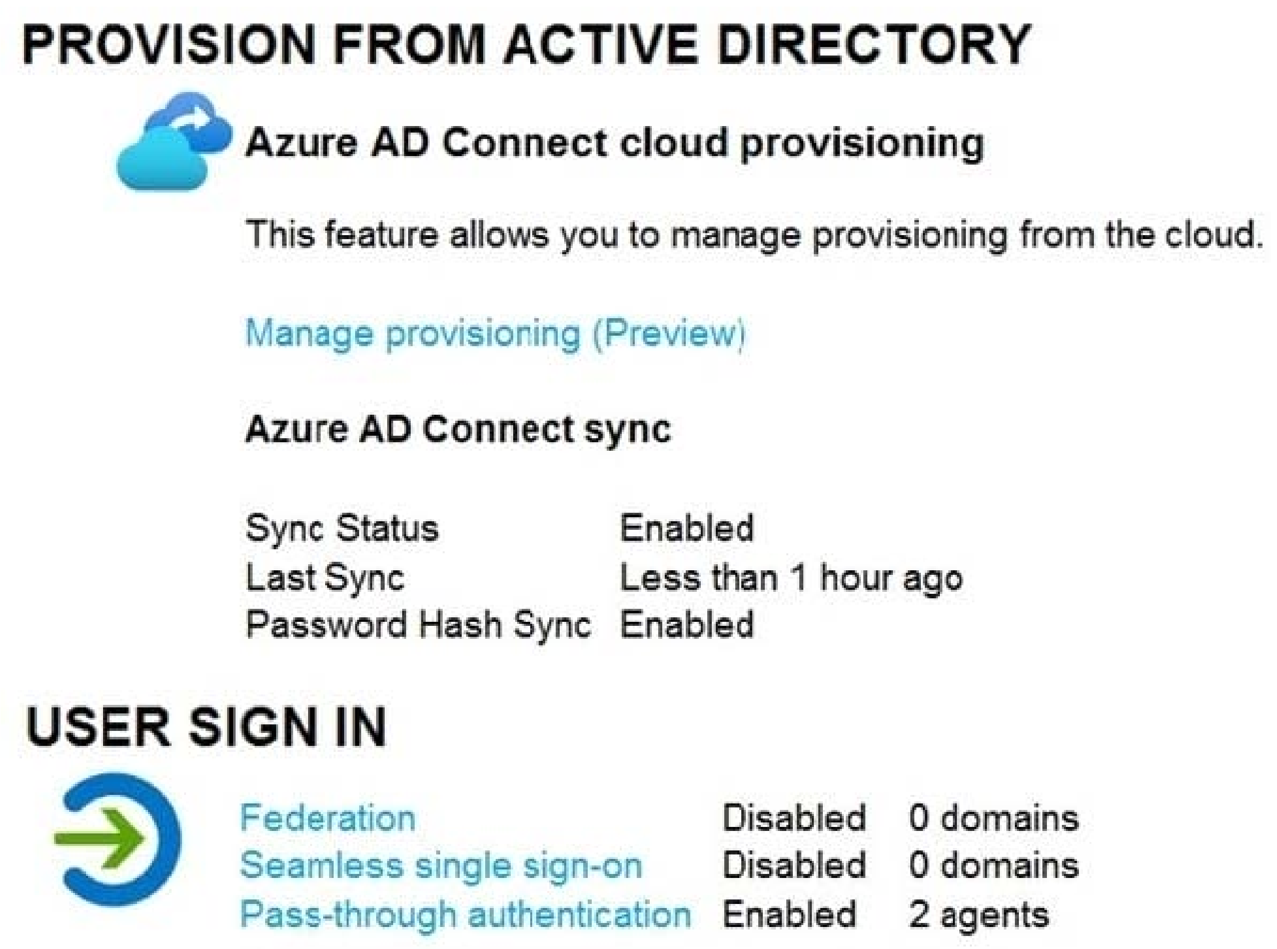
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.



Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.

Azure AD Connect is configured in Azure AD as shown in the following exhibit.



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

Connectivity from the on-premises domain to the internet is lost. Which users can sign in to Azure AD?

A. User1 only

B. User1 and User 3 only

C. User1, and User2 only

D. User1, User2, and User3

Correct Answer: B

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current-limitations#unsupported-scenarios

Read the Note:

Enabling Password Hash Synchronization gives you the option to failover authentication if your on-premises infrastructure is disrupted. This failover from Pass-through Authentication to Password Hash Synchronization is not automatic. You\\'ll

need to switch the sign-in method manually using Azure AD Connect. If the server running Azure AD Connect goes down, you\\'ll require help from Microsoft Support to turn off Pass-through Authentication.

Since the Password Hash sync failover is not automatic, in this case the answer is A. User2 that is directory sync will need Pass-Through Authentication, which will be unavailable at that moment.

QUESTION 3

You have a Microsoft 365 tenant.

You have an Active Directory domain that syncs to the Azure Active Directory {Azure AD) tenant.

Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.

What should you use to gather the information?

A. Cloud App Discovery in Microsoft Defender for Cloud Apps

B. enterprise applications in Azure AD

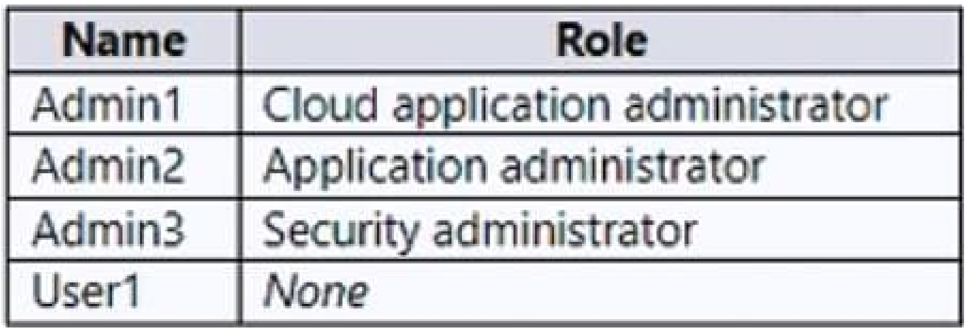
C. access reviews in Azure AD

D. Application Insights in Azure Monitor

Correct Answer: A

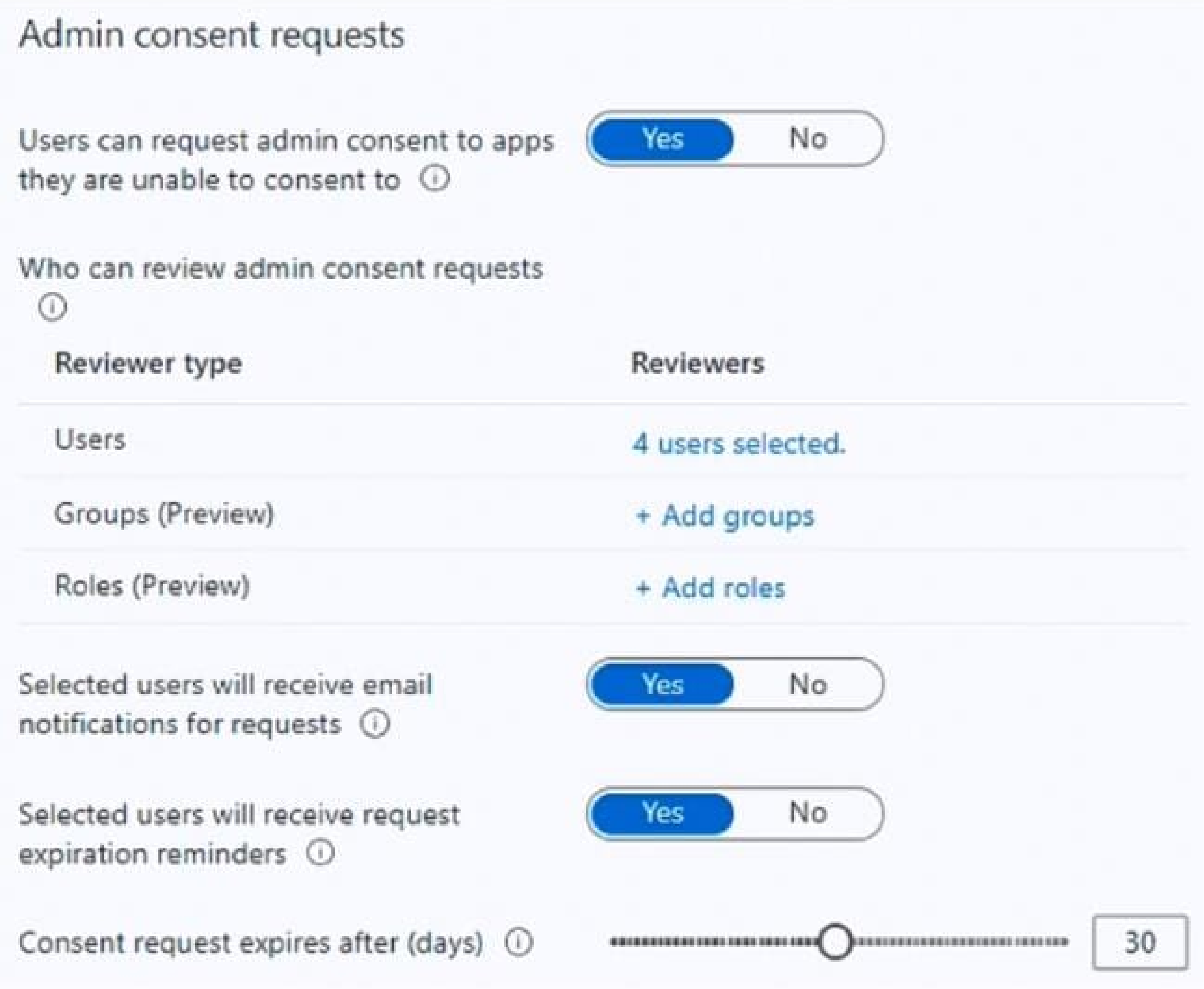
QUESTION 4

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



Name	Role
Admin1	Cloud application administrator
Admin2	Application administrator
Admin3	Security administrator
User1	*None*

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1. App1 requires admin consent to access Azure AD before the app can be used. You configure the Admin consent requests settings as shown in the following exhibit.



Admin consent requests

Users can request admin consent to apps they are unable to consent to ⓘ [✓ Yes] No

Who can review admin consent requests ⓘ

Reviewer type	Reviewers
Users	4 users selected.
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests ⓘ [✓ Yes] No

Selected users will receive request expiration reminders ⓘ [✓ Yes] No

Consent request expires after (days) ⓘ 30

Admin1, Admin2, Admin3, and User

Correct Answer: D

QUESTION 5

HOTSPOT

You have a Microsoft 365 tenant.

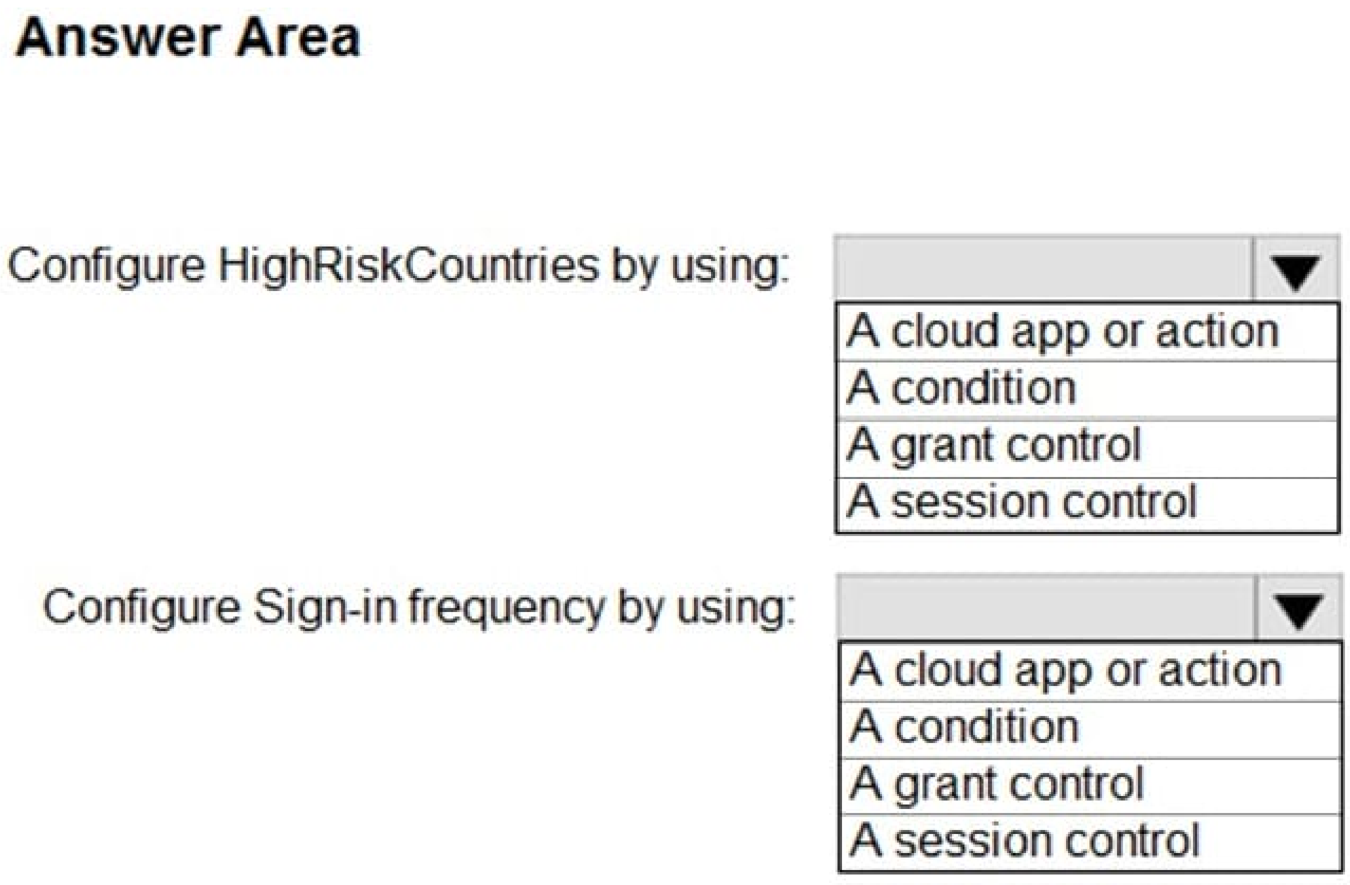
You create a named location named HighRiskCountries that contains a list of high-risk countries.

You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.

What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

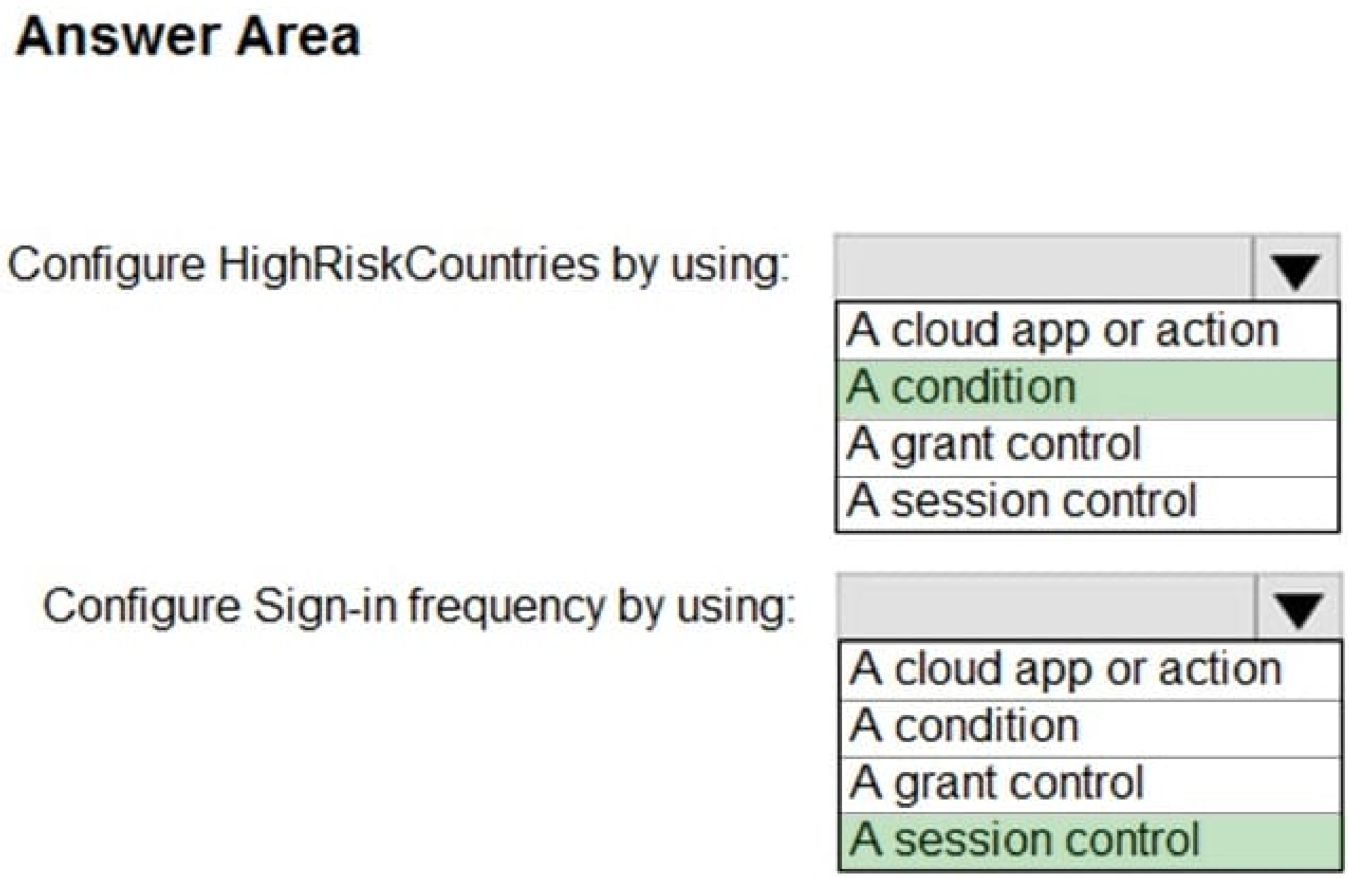
Configure HighRiskCountries by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Correct Answer:



Answer Area

Configure HighRiskCountries by using:

- A cloud app or action
- [✓ A condition]
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- [✓ A session control]

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session